UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

(Data Processing Agreement — DPA)

Wersja dokumentu: 1.2

Niniejsza Umowa powierzenia przetwarzania danych osobowych (dalej „**Umowa**") stanowi integralną część umowy o świadczenie usług drogą elektroniczną, na podstawie której Administrator korzysta z serwisu **TwójSzkrab** dostępnego pod adresem **twojszkrab.pl** oraz w postaci aplikacji mobilnej i przeglądarkowej (dalej łącznie „**Serwis**").

Umowa zostaje zawarta w formie elektronicznej (art. 28 ust. 9 RODO) z chwilą jej akceptacji przez osobę oświadczającą umocowanie do reprezentowania Administratora za pośrednictwem Serwisu i obowiązuje przez cały okres korzystania przez Administratora z Serwisu.

---

§ 1. Definicje i strony Umowy

1. **RODO** — Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.
2. **Procesor (Podmiot przetwarzający)** — operator Serwisu:

   __Wojciech Winkler__, prowadzący jednoosobową działalność gospodarczą pod firmą __Wojciech Winkler__, ul. Kminkowa 55 lok. 12, 51-180 Wrocław, wpisany do Centralnej Ewidencji i Informacji o Działalności Gospodarczej (CEIDG), __NIP 7811850983__, __REGON 366715416__, adres e-mail w sprawach ochrony danych: __kontakt@twojszkrab.pl__.
3. **Administrator** — podmiot prowadzący placówkę opieki nad dziećmi (żłobek, klub dziecięcy, przedszkole lub podobną placówkę), który zaakceptował niniejszą Umowę za pośrednictwem Serwisu. Administrator jest identyfikowany danymi wskazanymi w jego koncie w Serwisie (nazwa, NIP, adres). Umowa nie personalizuje tych danych w swojej treści — strony ustala się przez odesłanie do rekordu akceptacji oraz danych rejestrowych konta Administratora, których kompletność (nazwa, NIP oraz adres: ulica, numer, kod pocztowy, miejscowość) jest technicznym warunkiem akceptacji Umowy w Serwisie.
4. **Osoba, której dane dotyczą** — osoba fizyczna, której dane osobowe są przetwarzane w Serwisie (w szczególności dziecko, rodzic lub opiekun prawny, osoba upoważniona do odbioru dziecka, a także personel placówki).
5. **Dane osobowe** — dane osobowe w rozumieniu art. 4 pkt 1 RODO powierzone Procesorowi przez Administratora do przetwarzania w związku z korzystaniem z Serwisu.
6. **Podprzetwarzający (Subprocesor)** — dalszy podmiot przetwarzający, któremu Procesor powierza przetwarzanie danych osobowych zgodnie z § 6 Umowy.
7. Strony potwierdzają, że w zakresie danych przetwarzanych w Serwisie **Administrator jest administratorem danych** w rozumieniu art. 4 pkt 7 RODO, a **Procesor przetwarza je wyłącznie w jego imieniu** jako podmiot przetwarzający w rozumieniu art. 4 pkt 8 RODO.

---

§ 2. Przedmiot, charakter, cel i czas przetwarzania

1. **Przedmiot i cel powierzenia.** Administrator powierza Procesorowi przetwarzanie danych osobowych wyłącznie w celu i zakresie niezbędnym do świadczenia usług Serwisu, tj. prowadzenia elektronicznej ewidencji dzieci i obecności, komunikacji między placówką a rodzicami/opiekunami (wiadomości, ogłoszenia, ankiety), rozliczeń (należności) oraz obsługi kont użytkowników i powiadomień.

2. **Charakter przetwarzania.** Przetwarzanie odbywa się w sposób zautomatyzowany, w systemach teleinformatycznych Procesora i jego Podprzetwarzających, i obejmuje operacje takie jak: zbieranie, utrwalanie, przechowywanie, przeglądanie, porządkowanie, modyfikowanie, udostępnianie osobom uprawnionym w placówce oraz usuwanie danych. Przetwarzanie **nie obejmuje** zautomatyzowanego podejmowania decyzji wywołujących skutki prawne wobec osób, których dane dotyczą, ani profilowania w rozumieniu art. 22 RODO.

3. **Czas przetwarzania.** Procesor przetwarza dane przez okres obowiązywania umowy o świadczenie usług Serwisu, tj. przez czas korzystania przez Administratora z Serwisu, oraz — w zakresie opisanym w § 8 — przez czas niezbędny do ich zwrotu lub usunięcia po zakończeniu świadczenia usług. Zastrzeżenie stanowi retencja załączników, o której mowa w pkt 6, gdzie usunięcie następuje w toku obowiązywania Umowy.

4. Przedmiot, charakter, cel i czas przetwarzania są **jednakowe dla wszystkich Administratorów** korzystających z Serwisu, ponieważ usługa ma charakter jednorodny.

5. **Analiza sposobu korzystania z Serwisu.** Za udokumentowane polecenie Administratora, o którym mowa w § 4 pkt 1, uznaje się również analizowanie przez Procesora sposobu korzystania z Serwisu w celu zapewnienia jego prawidłowego działania i bezpieczeństwa, planowania pojemności oraz rozwoju funkcjonalności. Analiza taka podlega następującym ograniczeniom:

   a) prowadzona jest **wyłącznie w infrastrukturze wskazanej w § 5 ust. 1 lit. g**, bez udziału podmiotów trzecich i bez przekazywania danych poza tę infrastrukturę — Serwis **nie wykorzystuje zewnętrznych narzędzi analitycznych** wbudowanych w aplikacje klienckie;

   b) opiera się na zapisach dziennika aktywności (kto, kiedy i jakiej operacji dokonał) oraz na danych o charakterze ilościowym, i **nie obejmuje zapoznawania się z treścią komunikacji, wizerunkiem ani danymi szczególnych kategorii** w rozumieniu art. 9 RODO, o których mowa w § 3 ust. 2 lit. b, c i g;

   c) jej wyniki mają postać **zagregowaną i statystyczną**, niepozwalającą na identyfikację poszczególnych osób, których dane dotyczą;

   d) **nie służy** marketingowi, profilowaniu osób, których dane dotyczą, ani udostępnianiu jakichkolwiek danych podmiotom trzecim.

6. **Retencja załączników do wpisów.** Za udokumentowane polecenie Administratora, o którym mowa w § 4 pkt 1, uznaje się również **trwałe usuwanie przez Procesora plików** (zdjęć i dokumentów) dołączonych do wpisów w Serwisie, na następujących zasadach:

   a) plik jest usuwany wraz z kopiami po upływie **12 miesięcy** od jego opublikowania w Serwisie, chyba że Strony uzgodnią inny okres — uzgodniony okres Procesor odnotowuje w konfiguracji konta Administratora i stosuje w miejsce okresu domyślnego;

   b) usunięcie obejmuje **wyłącznie plik**; treść wpisu, komentarze oraz wyniki ankiet pozostają w Serwisie i podlegają § 8 na zasadach ogólnych;

   c) usuwanie **nie obejmuje wpisów przypiętych** przez Administratora lub upoważniony przez niego personel; odpięcie wpisu rozpoczyna bieg okresu, o którym mowa w lit. a, na nowo;

   d) usunięcie jest **nieodwracalne** — Procesor nie utrzymuje kopii pozwalającej na odtworzenie pliku po tym terminie;

   e) jeżeli przepisy prawa nakładają na Administratora obowiązek przechowywania danych zawartych w załącznikach przez okres dłuższy, **Administrator odpowiada za ich pobranie z Serwisu i zarchiwizowanie we własnym zakresie** przed upływem okresu retencji albo za uzgodnienie z Procesorem dłuższego okresu na podstawie lit. a. Serwis udostępnia Administratorowi termin wygaśnięcia każdego załącznika przed jego nastąpieniem;

   f) Administrator może w każdym czasie polecić Procesorowi zaprzestanie stosowania retencji dla swojego konta; polecenie takie Procesor wykonuje na zasadach lit. a.

Ograniczenie okresu przechowywania służy realizacji zasady ograniczenia przechowywania (art. 5 ust. 1 lit. e RODO) i zmniejszeniu skutków ewentualnego naruszenia ochrony danych.

Wyniki analizy w postaci zagregowanej i statystycznej nie stanowią danych osobowych i mogą być wykorzystywane przez Procesora również po zakończeniu obowiązywania Umowy.

---

§ 3. Rodzaj danych osobowych i kategorie osób

1. **Kategorie osób, których dane dotyczą:**
   a) dzieci objęte opieką placówki,
   b) rodzice i opiekunowie prawni dzieci,
   c) osoby upoważnione przez rodziców/opiekunów do odbioru dziecka,
   d) personel placówki korzystający z Serwisu (właściciele placówki, pracownicy).
2. **Rodzaj (kategorie) danych osobowych** przetwarzanych w Serwisie:
   a) **dane identyfikacyjne dzieci:** imię, nazwisko, **numer PESEL**, przezwisko/imię zdrobniałe, data urodzenia, data rozpoczęcia i zakończenia uczęszczania, przypisanie do placówki i grupy, notatki opisowe;
   b) **dane dotyczące zdrowia i sposobu żywienia dzieci** (szczególne kategorie danych w rozumieniu **art. 9 RODO**): informacje o diecie oraz dane wprowadzane w dziennym statusie dziecka — apetyt, samopoczucie (nastrój), informacje o wypróżnieniach, komentarze opiekunów, a także wszelkie informacje o stanie zdrowia wprowadzone przez Administratora w polach opisowych (notatka dziecka, komentarz do obecności, wiadomości);
   c) **wizerunek** — zdjęcia i inne pliki graficzne (formaty JPG/PNG) oraz dokumenty (PDF) publikowane w Serwisie jako załączniki do ogłoszeń i wpisów, w tym **zdjęcia przedstawiające dzieci**;
   d) **dane obecności:** data, godziny przyjścia i odbioru, status obecności, komentarze, wskazanie osoby odbierającej dziecko;
   e) **dane osób upoważnionych do odbioru:** imię, nazwisko, rodzaj pokrewieństwa/relacji, **numer dokumentu tożsamości**;
   f) **dane rodziców/opiekunów oraz personelu:** imię, nazwisko, adres e-mail, adres (ulica, numer, kod pocztowy, miejscowość, kraj), numer telefonu, dane uwierzytelniające (hasło wyłącznie w postaci skrótu kryptograficznego), przypisane role i uprawnienia;
   g) **treść komunikacji:** wiadomości między rodzicami a placówką, ogłoszenia, komentarze, ankiety i oddane w nich głosy, wraz z załącznikami;
   h) **dane rozliczeniowe:** pozycje należności, kwoty i statusy płatności związane z pobytem dziecka;
   i) **dane techniczne i eksploatacyjne:** identyfikatory urządzeń oraz **tokeny powiadomień push (FCM)**, adres IP i informacja o programie klienckim (user agent) utrwalane przy akceptacji dokumentów prawnych, a także zapisy dziennika aktywności (kto, kiedy i jakiej operacji dokonał, wraz z oznaczeniem działań wykonanych w trybie wsparcia technicznego).
3. Administrator oświadcza, że jest uprawniony do powierzenia powyższych danych, w tym danych szczególnych kategorii (art. 9 RODO) oraz wizerunku, i że dysponuje odpowiednią podstawą prawną ich przetwarzania — w szczególności odpowiednimi zgodami lub upoważnieniami rodziców i opiekunów prawnych w zakresie publikacji wizerunku dzieci. Procesor przetwarza dane szczególnych kategorii i wizerunek wyłącznie w zakresie, w jakim Administrator lub działający w jego imieniu użytkownicy wprowadzą je do Serwisu w ramach jego funkcjonalności.

4. Administrator zobowiązuje się nie wprowadzać do Serwisu danych osobowych wykraczających poza zakres niezbędny do korzystania z jego funkcjonalności, w szczególności w polach opisowych o charakterze swobodnego tekstu.

---

§ 4. Obowiązki Procesora

Procesor zobowiązuje się, zgodnie z art. 28 ust. 3 RODO, że:

1. **(polecenie Administratora)** przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora — za które uznaje się także korzystanie z funkcji Serwisu zgodnie z jego przeznaczeniem oraz niniejszą Umowę — w tym w zakresie przekazywania danych do państwa trzeciego lub organizacji międzynarodowej, chyba że obowiązek taki nakłada na Procesora prawo Unii lub prawo państwa członkowskiego; w takim przypadku Procesor informuje Administratora o tym obowiązku prawnym przed rozpoczęciem przetwarzania, o ile prawo to nie zabrania takiego informowania ze względu na ważny interes publiczny;
2. **(poufność)** zapewnia, by osoby upoważnione do przetwarzania danych zobowiązały się do zachowania poufności lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
3. **(bezpieczeństwo)** podejmuje środki techniczne i organizacyjne wymagane na mocy art. 32 RODO, opisane w § 5;
4. **(podprzetwarzający)** przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, o których mowa w art. 28 ust. 2 i 4 RODO oraz w § 6 Umowy;
5. **(prawa osób)** biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga Administratorowi — poprzez odpowiednie środki techniczne i organizacyjne — wywiązać się z obowiązku odpowiadania na żądania osób, których dane dotyczą, w zakresie wykonywania ich praw określonych w rozdziale III RODO;
6. **(wsparcie compliance)** uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga Administratorowi wywiązać się z obowiązków określonych w art. 32–36 RODO (bezpieczeństwo, zgłaszanie i zawiadamianie o naruszeniach, ocena skutków dla ochrony danych, uprzednie konsultacje);
7. **(zgłaszanie naruszeń)** zawiadamia Administratora o stwierdzonym naruszeniu ochrony powierzonych danych osobowych bez zbędnej zwłoki, nie później niż w ciągu **48 godzin** od jego wykrycia, przekazując informacje niezbędne Administratorowi do wykonania jego obowiązków z art. 33–34 RODO;
8. **(zwrot/usunięcie)** po zakończeniu świadczenia usług związanych z przetwarzaniem, zależnie od decyzji Administratora, usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa istniejące ich kopie, zgodnie z § 8, chyba że prawo Unii lub prawo krajowe nakazują dalsze przechowywanie danych;
9. **(rozliczalność i audyt)** udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO oraz umożliwia Administratorowi lub upoważnionemu przez niego audytorowi przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich, na warunkach określonych w § 7;
10. **(sygnalizacja niezgodnego polecenia)** niezwłocznie informuje Administratora, jeżeli jego zdaniem wydane polecenie stanowi naruszenie RODO lub innych przepisów o ochronie danych.

---

§ 5. Środki bezpieczeństwa (art. 32 RODO)

1. Procesor wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych, z uwzględnieniem stanu wiedzy technicznej, kosztów wdrożenia oraz charakteru, zakresu, kontekstu i celów przetwarzania. W szczególności Procesor stosuje:

a) **szyfrowanie transmisji** danych (protokół TLS) w komunikacji aplikacji klienckich z Serwisem;

b) **kontrolę dostępu opartą na rolach** (administrator systemu / właściciel placówki / pracownik / rodzic), tak by użytkownik miał dostęp wyłącznie do danych niezbędnych dla jego roli — w szczególności rodzic ma dostęp wyłącznie do danych własnego dziecka — oraz **logiczną izolację danych poszczególnych placówek** (architektura wielopodmiotowa);

c) **uwierzytelnianie** za pomocą tokenów sesyjnych o krótkim okresie ważności (10 minut), przechowywanych po stronie aplikacji klienckiej w zabezpieczonym magazynie systemu operacyjnego, oraz przechowywanie haseł wyłącznie w postaci skrótu kryptograficznego (funkcja BCrypt) — Procesor **nie przechowuje haseł w postaci jawnej** i nie ma do nich dostępu;

d) **rozliczalność i ślad audytowy** — rejestrowanie istotnych operacji na danych (dziennik aktywności), w tym **odrębne oznaczanie działań wykonywanych przez Procesora w trybie wsparcia technicznego** (dostęp do konta użytkownika w celu diagnostyki), przy czym taki dostęp nigdy nie jest wykorzystywany do składania oświadczeń woli w imieniu Administratora;

e) **kopie zapasowe** oraz środki zapewniające ciągłość działania i odtworzenie dostępu do danych w razie incydentu;

f) **monitorowanie błędów i incydentów** za pomocą narzędzi wskazanych w Wykazie Podprzetwarzających (§ 6);

g) przechowywanie danych powierzonych w infrastrukturze zlokalizowanej na terytorium **Europejskiego Obszaru Gospodarczego** — podstawowa infrastruktura Serwisu (baza danych, pliki, kolejki, monitoring) znajduje się w Polsce (region Warszawa) i w Niemczech.

2. Procesor okresowo testuje, mierzy i ocenia skuteczność wdrożonych środków oraz aktualizuje je stosownie do zmian w usłudze i stanu wiedzy technicznej.

---

§ 6. Podprzetwarzający (dalsze powierzenie)

1. Administrator udziela Procesorowi **ogólnej zgody** na korzystanie z usług dalszych podmiotów przetwarzających (Podprzetwarzających) w celu świadczenia usług Serwisu.

2. Aktualny **Wykaz Podprzetwarzających** stanowi **załącznik** do niniejszej Umowy i jest publikowany jako **odrębny, wersjonowany dokument** udostępniany za pośrednictwem Serwisu. Wykaz nie stanowi części treści niniejszej Umowy podlegającej akceptacji — jego zmiana **nie wymaga ponownej akceptacji Umowy**, a jedynie poinformowania Administratora i umożliwienia mu wniesienia sprzeciwu zgodnie z ust. 4.

3. Procesor zapewnia, że każdy Podprzetwarzający jest związany obowiązkami w zakresie ochrony danych **co najmniej równoważnymi** obowiązkom Procesora wynikającym z niniejszej Umowy, w szczególności obowiązkiem wdrożenia odpowiednich środków technicznych i organizacyjnych (art. 28 ust. 4 RODO).

4. Procesor informuje Administratora o zamierzonych zmianach dotyczących dodania lub zastąpienia Podprzetwarzających — poprzez aktualizację Wykazu udostępnianego w Serwisie — z co najmniej **30-dniowym** wyprzedzeniem, dając Administratorowi możliwość wyrażenia **sprzeciwu** wobec takich zmian. W razie zgłoszenia przez Administratora uzasadnionego sprzeciwu, którego Strony nie zdołają rozwiązać, Administrator jest uprawniony do wypowiedzenia umowy o świadczenie usług Serwisu.

5. Jeżeli Podprzetwarzający nie wywiąże się ze swoich obowiązków w zakresie ochrony danych, pełna odpowiedzialność wobec Administratora za wypełnienie obowiązków tego Podprzetwarzającego spoczywa na Procesorze.

6. Przekazywanie do państw trzecich. Dane powierzone są przechowywane w EOG. Jeżeli świadczenie wybranych funkcji Serwisu (w szczególności dostarczanie powiadomień push na urządzenia użytkowników) wiąże się z przekazaniem danych poza EOG, Procesor zapewnia, że odbywa się ono na

podstawie mechanizmu zgodnego z rozdziałem V RODO, w szczególności standardowych klauzul umownych zatwierdzonych przez Komisję Europejską. Zakres danych przekazywanych w treści powiadomień jest ograniczony do niezbędnego minimum.

---

§ 7. Prawo kontroli i audytu

1. Administrator ma prawo kontroli, czy Procesor przetwarza powierzone dane zgodnie z Umową i RODO.
2. Kontrola odbywa się w godzinach pracy Procesora, po uprzednim zawiadomieniu z co najmniej **14-dniowym** wyprzedzeniem, w sposób niezakłócający normalnej działalności Procesora oraz z poszanowaniem tajemnicy przedsiębiorstwa i danych innych klientów Serwisu.
3. Procesor może wykazać zgodność, o której mowa w ust. 1, również poprzez udostępnienie aktualnych certyfikatów, raportów z audytów lub opisu wdrożonych środków bezpieczeństwa.

---

§ 8. Zakończenie Umowy, zwrot i usunięcie danych

1. Umowa obowiązuje przez okres obowiązywania umowy o świadczenie usług Serwisu i ulega rozwiązaniu wraz z jej zakończeniem.
2. Po zakończeniu świadczenia usług Procesor — zależnie od decyzji Administratora wyrażonej nie później niż w terminie **30 dni** od zakończenia — **zwraca** dane osobowe Administratorowi (w powszechnie używanym formacie nadającym się do odczytu maszynowego) albo je **usuwa** wraz z istniejącymi kopiami. Brak decyzji Administratora w tym terminie uprawnia Procesora do usunięcia danych.
3. Procesor może zachować dane po zakończeniu Umowy wyłącznie w zakresie i przez czas wymagany przez prawo Unii lub prawo krajowe; w takim zakresie dane podlegają dalszej ochronie na zasadach określonych w Umowie.
4. Rekordy stanowiące dowód akceptacji dokumentów prawnych (w tym niniejszej Umowy) mają charakter rozliczeniowy (art. 5 ust. 2 RODO) i mogą być przechowywane niezależnie od powyższego przez okres niezbędny do wykazania spełnienia obowiązków oraz dochodzenia lub obrony roszczeń.

---

§ 9. Odpowiedzialność

1. Każda ze Stron odpowiada za szkody wyrządzone drugiej Stronie oraz osobom, których dane dotyczą, w związku z przetwarzaniem danych niezgodnym z Umową lub RODO, na zasadach określonych w art. 82 RODO i przepisach powszechnie obowiązujących.
2. Administrator ponosi odpowiedzialność za zgodność z prawem pozyskania danych powierzonych Procesorowi oraz za posiadanie podstawy prawnej ich przetwarzania, w tym danych szczególnych kategorii oraz wizerunku dzieci publikowanego w Serwisie.

---

§ 10. Postanowienia końcowe

1. Umowa zostaje zawarta w formie elektronicznej z chwilą jej akceptacji za pośrednictwem Serwisu przez osobę oświadczającą umocowanie do reprezentowania Administratora. Akceptacja jest utrwalana w Serwisie (data i godzina, wersja dokumentu, adres IP, identyfikacja konta i osoby akceptującej) i stanowi dowód zawarcia Umowy. Zapisy te mają charakter wyłącznie dowodowy i nie podlegają modyfikacji ani usunięciu.
2. Umowa wiąże **placówkę (Administratora)**, a nie osobę fizyczną, która dokonała akceptacji; ponowne uzyskanie akceptacji od kolejnego przedstawiciela tej samej placówki nie jest wymagane.

3. Zmiana treści Umowy następuje poprzez opublikowanie nowej, oznaczonej numerem wersji, i — o ile zmiana tego wymaga — ponowne pozyskanie akceptacji Administratora za pośrednictwem Serwisu. Opublikowanej wersji nie zmienia się; każda wersja jest archiwizowana odrębnie.
4. W sprawach nieuregulowanych Umową stosuje się przepisy RODO, ustawy o ochronie danych osobowych oraz Kodeksu cywilnego.
5. Prawem właściwym jest prawo polskie. Ewentualne spory rozstrzyga sąd właściwy miejscowo dla siedziby Procesora.

Dokument w wersji 1.1. Niniejszy tekst ma charakter ogólny (jednakowy dla wszystkich Administratorów); strony Umowy ustala się przez odesłanie do danych konta Administratora oraz rekordu akceptacji utrwalonego w Serwisie. Wykaz Podprzetwarzających jest publikowany jako odrębny, wersjonowany dokument (§ 6 ust. 2).